PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 5 :		(11) International Publication Number: WO 92/03000
H04L 9/00	A1	(43) International Publication Date: 20 February 1992 (20.02.92)

(21) International Application Number: PCT/US91/05386

(22) International Filing Date: 30 July 1991 (30.07.91)

(30) Priority data:

561,888	2 August 1990 (02.08.90)	US
666,896	8 March 1991 (08.03.91)	US

(71) Applicant: BELL COMMUNICATIONS RESEARCH, INC. [US/US]; 290 West Mount Pleasant Avenue, Livingston, NJ 07039-2729 (US).

(72) Inventors: HABER, Stuart, Alan ; 22 Irving Place, Apt. 2C, New York, NY 10003 (US). STORNETTA, Wakefield, Scott, Jr. ; 34 Harding Terrace, Morristown, NJ 07960 (US).

(74) Agents: WINTER, Richard, C.; PCT Int'l., Inc., c/o Bell Communications Research, Inc., International Coordinator, Room 2E-304, 290 West Mount Pleasant Avenue, Livingston, NJ 07039 (US) et al.

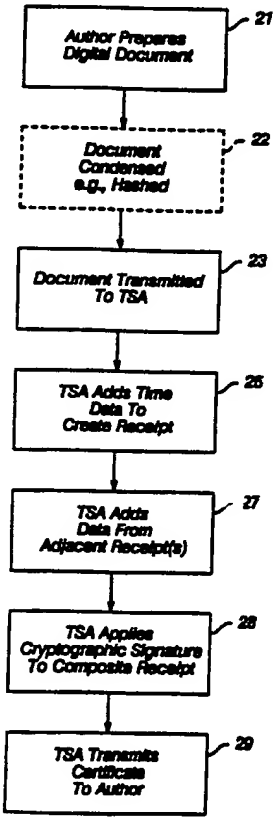
(81) Designated States: AT (European patent), BE (European patent), CA, CH (European patent), DE (European patent), DK (European patent), ES (European patent), FR (European patent), GB (European patent), GR (European patent), IT (European patent), JP, LU (European patent), NL (European patent), SE (European patent).

Published
With international search report.

(54) Title: METHOD FOR SECURE TIME-STAMPING OF DIGITAL DOCUMENTS

(57) Abstract

A system for time-stamping a digital document is disclosed which protects the secrecy of the document text and provides a tamper-proof time seal establishing an author's claim to the temporal existence of the document. Initially the author prepares the document (21), which may then be condensed by a process such as hashing (22). Next, the document is transmitted to the Time Stamping Authority (23), which adds time data to create a receipt (25) and data from adjacent receipts (27). Thereafter, the Time Stamping Authority applies a cryptographic signature to the composite receipt (28), which is then transmitted to the author (29).



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria	ES	Spain	MG	Madagascar
AU	Australia	FI	Finland	ML	Mali
BB	Barbados	FR	France	MN	Mongolia
BE	Belgium	GA	Gabon	MR	Mauritania
BF	Burkina Faso	GB	United Kingdom	MW	Malawi
BG	Bulgaria	GN	Guinea	NL	Netherlands
BJ	Benin	GR	Greece	NO	Norway
BR	Brazil	HU	Hungary	PL	Poland
CA	Canada	IT	Italy	RO	Romania
CF	Central African Republic	JP	Japan	SD	Sudan
CG	Congo	KP	Democratic People's Republic of Korea	SE	Sweden
CH	Switzerland			SN	Senegal
CI	Côte d'Ivoire	KR	Republic of Korea	SU+	Soviet Union
CM	Cameroon	LI	Liechtenstein	TD	Chad
CS	Czechoslovakia	LK	Sri Lanka	TG	Togo
DE	Germany	LU	Luxembourg	US	United States of America
DK	Denmark	MC	Monaco		

+ **It is not yet known for which States of the former Soviet Union any designation of the Soviet Union has effect.**

METHOD FOR SECURE TIME-STAMPING OF DIGITAL DOCUMENTS

BACKGROUND OF THE INVENTION

In many situations there is a need to establish the date on which a document was created and to prove that the text of a document in question is in fact the same as that of the original dated document. For example, in intellectual property matters it is often crucial to verify the date on which a person first put into writing the substance of an invention. A common procedure for thus "time-stamping" an inventive concept comprises daily notations of one's work in a laboratory notebook. Indelibly dated and signed entries are made one after another on each page of the notebook where the sequentially numbered, sewn-in pages make it difficult to revise the record without leaving telltale signs. The validity of the record is further enhanced by the regular review and signed witnessing by a generally disinterested third party. Should the time of the concept become a matter for later proof, both the physical substance of the notebook and the established recording procedure serve as effective evidence in substantiating the fact that the concept existed at least as early as the notebook witness date.

The increasingly widespread use of electronic documents, which include not only digital representations of readable text but also of video, audio, and pictorial data, now poses a serious threat to the viability of the "notebook" concept of establishing the date of any such document. Because electronic digital documents are so

easily revised, and since such revisions may be made without telltale sign, there is available limited credible evidence that a given document truly states the date on which it was created or the message it originally carried. For the same reasons there even arises serious doubt as to the authenticity of a verifying signature. Without an effective procedure for ensuring against the surreptitious revision of digital documents, a basic lack of system credibility prevents the efficiencies of electronic documentation from being more widely implemented.

Some procedures are presently available for verifying electronic document transmissions; however, such procedures are limited in application to bilateral communications. That is, in such communications the sender essentially desires to verify to the receiver the source and original content of the transmitted document. For example, "private key" cryptographic schemes have long been employed for message transmission between or among a limited universe of individuals who are known to one another and who alone know the decrypting key. Encryption of the message ensures against tampering, and the fact that application of the private key reveals the "plaintext" of the transmitted message serves as proof that the message was transmitted by one of the defined universe. The time of creation of the message is only collaterally established, however, as being not later than its receipt by the addressee. This practice thus fails to provide time-stamp evidence that would be useful in an unlimited universe at a later date.

A more broadly applicable verifying communication procedure, that of "public key" cryptography, has been described by Diffie and Hellman ("New Directions in Cryptography", IEEE Transactions On Information Theory,

Vol. IT-22, November 1976, pp. 644-654) and more recently implemented by Rivest et al. in U.S. Patent 4,405,829, issued 20 September 1983. While this scheme expands the utilizing universe to a substantially unlimited number of system subscribers who are unknown to one another, but for a public directory, verifiable communications remain bilateral. These limitations persist, since although a public key "signature", such as that which entails public key decryption of a message encrypted with the private key of the transmitter, provides any member of the unlimited universe with significant evidence of the identity of the transmitter of the message, only a given message recipient can be satisfied that the message existed at least as early as the time of its receipt. Such receipt does not, however, provide the whole universe with direct evidence of time of the message's existence. Testimony of a such a recipient in conjunction with the received message could advance the proof of message content and time of its existence, but such evidence falls victim to the basic problem of ready manipulation of electronic digital document content, whether by originator or witness.

Thus, the prospect of a world in which all documents are in easily modifiable digital form threatens the very substance of existing procedures for establishing the credibility of such documents. There is clearly a significant present need for a system of verification by which a digital document may be so fixed in time and content that it can present, at least to the extent currently recognized in tangible documents, direct evidence on those issues.

SUMMARY OF THE INVENTION

The present invention yields such a reliable system in a method of time-stamping digital documents that provides the equivalent of two essential characteristics of accepted document verification. First, the content of a document and a time stamp of its existence are "indelibly" incorporated into the digital data of the document so that it is not possible to change any bit of the resulting time-stamped data without such a change being apparent. In this manner, the state of the document text is fixed at the instant of time-stamping. Second, the time at which the digital document is stamped is verified by a "witnessing" digital signature procedure that deters the incorporation of a false time statement. In essence, the method transfers control of the time-stamping step from the author to an independent agent and removes from the author the ability to influence the agent in the application of other than a truthful time stamp.

The method of the present invention presumes a number of document authors distributed throughout a communication network. Such authors may be individuals, companies, company departments, etc. each representing a distinct and identifiable, e.g. by ID number or the like, member of the author universe. In one embodiment of the invention, this universe may constitute the clientele of a time-stamping agency (TSA), while in another embodiment the distributed authors may serve as agents individually performing the time-stamping service for other members of the universe.

In its general application, as depicted in FIG. 1 of the drawing, the present method entails an author's

preparation of a digital document, which may broadly comprise any alphanumeric, audio, or pictorial presentation, and the transmission of the document, preferably in a condensed representative form, to the TSA. The TSA time-stamps the document by adding digital data signifying the current time, applying the agency's cryptographic signature scheme to the document, and transmitting the resulting document, now a certificate of the temporal existence of the original document, back to the author where it is held for later use in required proof of such existence. Alternatively, the TSA may time-stamp the document to create a receipt by adding digital data signifying the current time, concatenate the receipt with the current cryptographic catenation of its prior time stamp receipts, and create a new catenation from the composite document by means of a deterministic function, such as discussed in greater detail below. The resulting catenate value is then included with time and other identifying data to yield the certificate.

To ensure against interception of confidential document information during transmission to the TSA, and to reduce the digital bandwidth required for transmission of an entire document, the author may optionally convert the digital document string to a unique value having vastly condensed digital size by means of a deterministic function which may, for example, be any one of a number of algorithms known in the art as "one-way hash functions". Such an application of hash functions has been described, among others, by Damgard in his discussions on the improvement of security in document signing techniques ("Collision-Free Hash Functions and Public Key Signature Schemes", Advances in Cryptology -- Eurocrypt '87, Springer-Verlag, LNCS, 1988, Vol. 304, pp. 203-217). In practice of the present invention, however, the "one-way"

characteristic typical of a hashing algorithm serves an additional purpose; that is, to provide assurance that the document cannot be secretly revised subsequent to the time the TSA applies its time stamp or incorporates the document into the catenate certificate.

A hashing function provides just such assurance, since at the time a document, such as an author's original work or a composite receipt catenation, is hashed there is created a representative "fingerprint" of its original content from which it is virtually impossible to recover that document. Therefore, the time-stamped document is not susceptible to revision by any adversary of the author. Nor is the author able to apply an issued time-stamp certificate to a revised form of the document, since any change in the original document content, even to the extent of a single word or a single bit of digital data, results in a different document that would hash to a completely different fingerprint value. Although a document cannot be recovered from its representative hash value, a purported original document can nonetheless be proven in the present time-stamping procedure by the fact that a receipt comprising a true copy of the original document representation will always hash to the original number or the same catenate value as is contained in the author's certificate, assuming use of the original hashing algorithm.

Any available deterministic function, e.g. a one-way hash function such as that described by Rivest ("The MD4 Message Digest Algorithm", Advances in Cryptology -- Crypto '90, Springer-Verlag, LNCS, to appear), incorporated herein by reference, may be used in the present procedure. In the practice of the invention, such a hashing operation is optionally employed by the author

to obtain the noted benefit of transmission security, although it might be effected by the TSA if the document were received in plaintext form. In whatever such manner the document content and incorporated time data are fixed against revision, there remains the further step, in order to promote the credibility of the system, of certifying to the members of an as yet unidentified universe that the receipt was in fact prepared by the TSA, rather than by the author, and that the time indication is correct, i.e., that it has not, for instance, been fraudulently stated by the TSA in collusion with the author.

To satisfy the former concern, the TSA uses a verifiable signature scheme, of a type such as the public key method earlier noted, to certify the time-stamp prior to its transmittal to the author. Confirmation of the signature at a later time, such as by decryption with the TSA's public key, proves to the author and to the universe at large that the certificate originated with the TSA. Proof of the veracity of the time-stamp itself, however, relies upon a following additional aspect of the invention.

In an alternative procedure, the TSA maintains a record of its sequential time-stamping transactions by adding each new receipt to its current catenation and applying its deterministic function, e.g. hashing, the composite to obtain a new catenation. This catenation, itself a value resulting from the hashing process, is included on the receipt or certificate returned to the author and serves to certify the indicated time stamp. Confirmation of the certificate at a later time involves rehashing the combination of the author's time receipt and the next previous catenate value in the TSA records. The resulting generation of the author's catenate certificate

value proves to the author and to the universe at large that the certificate originated with the TSA. This result also proves the veracity of the time-stamp itself, since all original elements of the original receipt must be repeated in order to again generate, by the hashing function, the original catenate certificate value.

One embodiment of the process, as generally depicted in FIG. 2, draws upon the relatively continuous flow of documents from the universe of authors through the facilities of the TSA. For each given processed document, D_k, the TSA generates a time-stamp receipt which includes, for example, a sequential receipt number, r_k, the identity of the author, A_k, by ID number, ID_k, or the like, the hash, H_k, of the document, and the current time, t_k. In addition, the TSA includes the receipt data of the immediately preceding processed document, D_{k-1}, of author, A_{k-1}, thereby bounding the time-stamp of document, D_k, in the "past" direction by the independently established earlier receipt time, t_{k-1}. Likewise, the receipt data of the next received document, D_{k+1}, are included to bound the time-stamp of document, D_k, in the "future" direction. The composite receipt, now containing the time data of the three, or more if desired, sequential time-stamp receipts, or identifying segments thereof, is then certified with the cryptographic TSA signature and transmitted to the author, A_k. In like manner, a certificate containing identifiable representations of D_k and D_{k+2} would be transmitted to author, A_{k+1}. Thus, each of the time-stamp certificates issued by the TSA is fixed in the continuum of time and none can be falsely prepared by the TSA, since a comparison of a number of relevant distributed certificates would reveal the discrepancy in their sequence. So effective is such a sequential fixing of a document in the time stream that the TSA signature could

be superfluous in actual practice.

A second embodiment of the invention, shown generally in FIG. 3, distributes the time-stamping task randomly among a broad universe, for example the multiplicity of authors utilizing the time-stamping process. A TSA could still be employed for administrative purposes or the requesting author could communicate directly with the selected time-stamping author/agents. In either event, the above-mentioned need for assurance that a time-stamp has not been applied to a document through collusion between the author and the stamping agency is met in the combination of the reasonable premise that at least some portion of the agency universe is incorruptible or would otherwise pose a threat of exposure to an author attempting falsification, and the fact that the time-stamping agencies for a given document are selected from the universe entirely at random. The resulting lack of a capability on the part of the author to select a prospective collusive agent of the author's own choosing substantially removes the feasibility of intentional time falsification.

The selection of the individual universe members who will act as the predetermined number of agents is accomplished by means of a pseudorandom generator of the type discussed by Impagliazzo, Levin, and Luby ("Pseudorandom Generation From One-Way Functions", Proc. 21st STOC, pp. 12-24, ACM, 1989) for which the initial seed is a deterministic function, such as a hash, of the document being time-stamped. Given as a seed input the document hash or other such function, the implemented pseudorandom generator will output a series of agency IDs. This agency selection is for all practical purposes unpredictable and random.

Once the agents are selected, the time-stamping proceeds as previously indicated with the exception that each agent individually adds the current time data to the representative document it receives, certifies the resulting separate time-stamped receipt with its own verifiable cryptographic signature, and transmits the certificate back to the author. This transmittal may be directly to the requesting author or by way of the administrative TSA where the receipts are combined with or without further certification by the TSA. The combination of signature scheme and a published directory of author IDs provides verification of the utilization of the agents that were in fact selected by the pseudorandom generator. This distributed agent embodiment of the invention presents some advantages over the receipt-linking procedure in that a certified time-stamp is provided more quickly and a given author's later proof of a document is less reliant upon the availability of the certificates of other authors.

In an additional embodiment shown in FIG. 4, the TSA generates a time-stamp receipt which includes, for example, a sequential receipt transaction number, r_k, the identity of the author, for example by ID number, ID_k, or the like, a digital representation, e.g. the hash, H_k, of the document, and the current time, t_k. The TSA then includes these receipt data, or any representative part thereof, with the catenate certificate value, C_{k-1}, of the immediately preceding processed document, D_{k-1}, of author, A_{k-1}, thereby bounding the time-stamp of document, D_k, by the independently established earlier receipt time, t_{k-1}.

The composite data string, $(r_k, ID_k, H_k, t_k, C_{k-1})$, is then hashed to a new catenate value, C_k, that is entered with transaction number, r_k, in the records of the TSA,

and is also transmitted to A_k, as the catenate certificate value, with the time-stamp receipt data. In like manner, a certificate value derived from the hashing of C_k with time stamp elements of the receipt for document, D_{k+1}, would be transmitted to author, A_{k+1}. Thus, each of the time-stamped catenate certificates issued by the TSA is fixed in the continuum of time and none can be falsely prepared by the TSA, since any attempt to regenerate a catenate certificate number from a hash with the next prior certificate would reveal the discrepancy.

In a more general application of the invention, as shown in FIG. 5, the representation, e.g., a hash, of a particular document is simply concatenated with the catenate certificate value of the next previous document and the deterministic function representation, again a hash, for example, of this composite is then generated and retained as the record catenate value for the particular document. Each subsequent document in the growing series is similarly processed to expand the record which itself would serve as a reliable certification of the position each such document occupies in the series, or more broadly viewed, in the continuum of time. This embodiment of the invention provides a reliable method by which an organization, for instance, could readily certify the sequence and continuity of its digital business documents and records.

Additional variations in the process of the invention might include the accumulation of documents, preferably in hashed or other representative form, generated within an author organization over a period of time, e.g. a day or more depending upon the extent of activity, with the collection being hashed to present a single convenient document for time-stamping and

certification. Also, the initial seed for the pseudorandom generator may be based upon a function of time or previously receipted documents, as well as of the document. As an alternative, an organizational designee might serve as a resident "outside" agency who would maintain a catenate certificate record of organization documents by means of the present procedure and on a regular basis would transmit the then current catenate certificate to a TSA. In this manner the sequence of an organization's business records would be established both within the organization and externally through the TSA.

Also, the implementation of process embodiments might readily be automated in simple computer programs which would directly carry out the various steps of hashing, transmitting, and concatenating original document representations, applying current time stamps, generating and recording catenate certificate values, and providing receipt certificates.

THE DRAWING

The present invention will be described with reference to the accompanying drawing of which:

FIG. 1 is a flow diagram of a general process of time-stamping a document according to the invention;

FIG. 2 is a flow diagram of a specific embodiment of the process;

FIG. 3 is a flow diagram of another specific

embodiment of the process;

FIG. 4 is a flow diagram of an alternative embodiment of the time-stamping process; and

FIG. 5 is a flow diagram of a general catenation process according to the invention.

DESCRIPTION OF THE INVENTION

The following examples of the application of embodiments of the present invention will serve to further describe the involved process. For convenience in the presentation of these examples, the deterministic function selected is the md4 hashing algorithm described by Rivest, as mentioned above, and the verifiable signature scheme is the public key method suggested by Diffie and Hellman, as implemented by Rivest et al. in U.S. Patent 4,405,829. The function actually selected by a TSA could be any of various available algorithms. Whatever algorithm is implemented, records of its identity and period of use must be maintained for later proof of certified receipts. Further, in order to simplify explanation of the process and for the additional reasons noted below, only representative segments of the entire numbers will be employed.

The receipt-linking embodiment of the invention shown in FIG. 2 is initially considered. Although the present process may be used with documents of any length, the following apt excerpt is amply representative of a

document, D_k, which an author prepares at step 21 and for which time-stamping is desired:

> Time's glory is to calm contending kings,
> To unmask falsehood, and bring truth to light,
> To stamp the seal of time in aged things,
> To wake the morn, and sentinel the night,
> To wrong the wronger till he render right;
>
> The Rape of Lucrece

By means of the md4 algorithm, the document is hashed, at optional, dashed step 22 to a number, H_k, of a standard 128 bit format which expressed in base 16 appears as:

ef6dfdcd833f3a43d4515a9fb5ce3915

The author, A_k, whose system identification number, ID_k, is 172 in a 1000 member author universe, transmits the thus-identified document to the system TSA, at step 23, as the message, (ID_k, H_k), which appears:

172, ef6dfdcd833f3a43d4515a9fb5ce3915

as a request that the document be time-stamped.

The TSA then prepares the receipt for document, D_k, by adding, at step 25, a sequential receipt number, r_k, of 132, for example, and a statement of the current time, t_k. This time statement might include a standard 32 bit representation of computer clock time plus a literal statement, i.e. 16:37:41 Greenwich Mean Time on 10 March 1990, in order to allow the final time-stamp certificate to be easily readable by the author, A_k. The receipt

would then comprise the string, (r_k, t_k, ID_k, H_k).

At this point it would be appropriate to further consider the earlier-mentioned reduction of number size to representative segments. As is described by Rivest et al. in U.S. Patent 4,405,829, the cryptographic public key scheme to be employed in this example (generally known in the field as the "RSA" signature scheme) requires the division of an extended message into blocks that may each be represented by a number not exceeding the encoding key number element, n. Each such block is then signed with the RSA algorithm, to be reassembled after transmission. Therefore, in order to be able to use a number, n, of reasonable size in this example while maintaining a single block for the final receipt string to be certified with the RSA scheme, each element of the receipt string will be reduced to a representative eight bits, typically the last eight bits of any overlong string, and those bits will be stated in base 16 to present a two hexadecimal character string. Thus, for instance, the 128 bit document hash, H_k, will be represented by its last eight bits, i.e. 0001 0101, stated as 15 (base 16). Likewise, ID_k, 172, is 1010 1100 and is represented by ac (base 16). Without actually undertaking the calculation, it will suffice to assume that the time statement, t_k, is represented as 51. The receipt number, 132, would be represented as 84. The receipt string to this point, i.e. (r_k, t_k, ID_k, H_k) now appears as 8451ac15.

Assume now that the immediately preceding document, D_{k-1}, was processed by the TSA as the request:

201, d2d67232a61d616f7b87dc146c575174

at 16:32:30 on 10 March 1990 (t_{k-1} being represented as

64). The TSA adds these data, at step 27, to the receipt string for D_k to yield the hexadecimal representation, 8451ac1564c974. This receipt, R_k, now contains data fixing the time for D_k and a time, t_{k-1}, before which author, A_k, cannot claim that D_k existed. This limitation on A_k is established by the fact that the previous author, A_{k-1}, holds a time certificate, C_{k-1}, that fixes t_{k-1} as subsequent to the linked time data, t_{k-2}, in the certificate of author, A_{k-2}, and so on for as long as a proof requires.

To establish that TSA in fact originated the receipt for document, D_k, that receipt is transmitted, at step 29, to author, A_k, after TSA signing, at step 28, with the public key cryptographic signature scheme and becomes the certified receipt, or certificate, C_k. With the data derived above, and assuming that TSA has the RSA signature key set, in decimal:

<n,e> = <43200677821428109,191> (Public)
<n,d> = <43200677821428109,29403602422449791> (Private)
the signed certificate for R_k, 8451ac1564c974, would compute as:

$$R^d \bmod n = 39894704664774392$$

When author, A_k, receives this certificate, C_k, along with the literal statement of R_k, it may be readily confirmed as being correct by application of the TSA public key to verify that:

$$C_k^e \bmod n = R_k$$

and that R_k in fact contains the data representing the document hash, H_k.

The procedure shown in this simple one-link example results in a certificate which, being bounded in time by the data from document, D_k, provides author, A_{k-1} with reliable evidence that document, D_{k-1}, was not backdated to a time significantly prior to the existence of document, D_k. When the certificate of A_k is expanded with additional data from the subsequently processed document, D_{k+1}, it will likewise be effectively bounded to substantiate the time stamp claimed by A_k. In an alternative of the same effect, A_k could simply be advised of the identity of A_{k+1} and could confirm from that author that the one-link certificate, C_{k+1}, contained the element, H_k. The procedure could also be varied to provide certified receipts which include data from any number of authors, with each addition providing a further degree of assurance against falsification.

Another embodiment of the invention, as shown in FIG. 3, which utilizes randomly selected members of the author universe as time-stamping agents, or witnesses, i.e. a "distributed trust" procedure, would proceed in the following manner. Although these numbers are not so limited in actual practice, for purposes of the example it will be assumed that the universe consists of 1000 authors, having IDs 0-999, and that three witnesses will be sufficient to establish the veracity of the time stamp. Also, in this example the earlier-noted variation including the services of a TSA is being implemented. The hashing function, md4, utilized in the above example is employed here also, in optional step 32, as an example of a deterministic document function which will seed the pseudorandom selection of the three witnesses from the author universe.

As in the previous example, the author transmits

the document to the TSA, normally in hashed form, as the identified request:

172, ef6dfdcd833f3a43d4515a9fb5ce3915

The TSA now uses this document hash string, in step 33, as the seed to generate the ID number of the first witness, at step 35, according to the selection algorithm:

ID = [md4 (seed)] mod (universe size)

The resulting seed hash:

26f54eae92511dbb5e06e7c2de6e0fcf

represents the 128 bit number which mod 1000 is 487, the ID of the first selected witness. The next witness is likewise chosen using this seed hash representation as the seed in the second selection computation to yield:

882653ee04d16b1f0d604883aa27300b

which mod 1000, is 571, the second witness ID. A repeat of the computation, again seeding with the prior seed hash, selects the final witness as 598, which is:

2fe8768ef3532f15c40acf1341902c1e mod 1000

The TSA now sends, at step 37, a copy of the original request to each of these three witnesses who individually, at step 38, add a current time statement and ID, and certify the resulting receipts by signing with the RSA cryptographic signature scheme and transmitting them, at step 39, directly to the author or through the TSA who may assemble the certificates into a file to be delivered

to the author. By virtue of the fact that the pseudorandom generation prevents the exercise of a personal choice in the selection of witnesses, the author is deterred by the risk of encountering a non-cooperative witness from attempting any communication prior to time stamp certification for the purpose of arranging for a false time entry. In a process variant where the author is allowed to transmit the request directly to witnesses, the random selection of such witnesses which is keyed essentially to the involved document itself frustrates any attempt by the author to direct the document to a known cooperative witness. The group of resulting certificates may thus be employed with confidence in later proofs employing signature verification in the manner earlier described.

The catenate certificate embodiment of the time-stamping procedure begins, as at step 41 in FIG. 4 of the drawing, with the preparation of a digital document by the author, e.g. A_k. As previously noted, this digital document may be the digital form or representation of any alphanumeric text or video, audio, pictorial or other form of fixed data. Although the present process may be used with documents of any length, the following excerpt is amply representative of a document, D_k, for which time-stamping is desired:

> ... the idea in .nich affirmation of the world and ethics are contained side by side ... the ethical acceptance of the world and of life, together with the ideals of civilization contained in this concept ... truth has no special time of its own. Its hour is now -- always.
>
> Schweitzer

If the author so desires, the document, D_k, may, for the purposes of security as well as to reduce the required transmission bandwidth, be condensed by means, for example, of the md4 algorithm. As indicated by the optional, dashed step 42, the document is thus hashed to a value, H_k, of a standard 128 bit format which, expressed in base 16, appears as:

ee2ef3ea60df10cb621c4fb3f8dc34c7

It should be noted at this point that the hexadecimal and other numerical value representations used in this example are not in such form crucial to the implementation of the invention. That is to say, any portion or other distinct representation of those values selected according to a given procedure would function as well.

Author, A_k, whose assigned identification number, ID_k, is 634 in a 1000 member author universe, then transmits the document, at step 43, to the system TSA in the identifying message, (ID_k, H_k), which appears:

634, ee2ef3ea60df10cb621c4fb3f8dc34c7

as a request that the document be time-stamped.

The TSA, at step 44, prepares the receipt for document, D_k, by adding a sequential receipt transaction number, r_k, of 1328, for example, and a statement of the current time, t_k. This time statement might be a standard binary representation of computer clock time or simply a literal statement, e.g., 19:46:28 Greenwich Mean Time on 6 March 1991, in order to allow the final time-stamp certificate to be easily read. The receipt then comprises the string, (r_k, t_k, ID_k, H_k), which appears as follows:

1328, 194628GMT06MAR91, 634,
ee2ef3ea60df10cb621c4fb3f8dc34c7

In accordance with the invention, the records of the TSA at this time contain a catenation of all its prior receipt transactions in the form, for example, of the values resulting from the hashing of each consecutive receipt with the record catenation to that time. This catenate record would thus have been developed as follows. The receipt of first transaction ($r_k = 1$) was hashed with an initial datum value, e.g., the hash of the identification of the TSA, to yield the first catenate value, C_1, which was then used as the certificate value for that first transaction. In the next transaction, the receipt was concatenated with C_1 and the composite hashed to yield the second catenate certificate value, C_2, and so on through the entire history of the TSA time-stamping operation.

Assume now that the document, D_{k-1}, immediately preceding that of the present example had been processed by the TSA, in its 1327th receipt transaction, to yield as the catenate certificate value, C_{k-1}:

26f54eae92516b1f0d6047c2de6e0fcf

In step 45 of the process, the TSA now concatenates with this value the receipt for D_k to obtain:

26f54eae92516b1f0d6047c2de6e0fcf, 1328,
194628GMT06MAR91, 634, ee2ef3ea60df10cb621c4fb3f8dc34c7

This composite is then hashed by the TSA, at step 46, to

yield as the new catenate certificate value, C_k:

46f7d75f0fbea95e96fc38472aa28ca1

The TSA then adds this value to its records and prepares and transmits to author, A_k, at step 47, a time-stamp certificate, including this catenate certificate value, which might appear as:

Transaction Number: 1328
Client ID Number: 634
Time: 19:46:28 Greenwich Mean Time
Date: 06 March 1991
Certificate Number: 46f7d75f0fbea95e96fc38472aa28ca1

The procedure would be repeated by the TSA for each subsequent time stamp request. Assuming the next request from A_{k+1} was received with the document in the form of its hash, H_{k+1}, as:

201, 882653ee04d511dbb5e06883aa27300b

at 19:57:52 GMT on 6 March 1991, the composite concatenation would appear:

46f7d75f0fbea95e96fc38472aa28ca1, 1329,
195752GMT06MAR1991, 201, 882653ee04d511dbb5e06883aa27300b

and the certificate returned to A_{k+1} would read:

Transaction Number: 1329
Client ID Number: 201
Time: 19:57:52 Greenwich Mean Time
Date: 06 March 1991
Certificate Number: d9bb1b11d58bb09c2763e7915fbb83ad

When, at a later date, author, A_{k+1}, desires to prove the authenticity of document, D_{k+1}, as that which was received and dated by the TSA on 6 March 1991 at 19:57:52, the records of the TSA are examined to obtain the catenate certificate value, C_k, of the next previous transaction, 1328, which appears as:

46f7d75f0fbea95e96fc38472aa28ca1

The alleged document is then reduced to the form in which it was transmitted to the TSA, e.g, as its hash, and this value is then concatenated with C_k and the remaining data from the certificate of A_{k+1}. The resulting composite, assuming the alleged document to be authentic, now appears as:

46f7d75f0fbea95e96fc38472aa28ca1, 1329,
195752GMT06MAR1991, 201, 882653ee04d511dbb5e06883aa27300b

which, when hashed, produces the correct catenate certificate value:

d9bb1b11d58bb09c2763e7915fbb83ad

thereby proving the alleged document to be D_{k+1}. Otherwise, a revised document would hash to a different value and the composite of which it is an element would hash to a catenate certificate value different from that stated in the certificate of transaction number 1329.

If further proof were demanded, for example upon an adversary allegation that C_{k+1} had been falsified after the fact of a document revision, the certificate and the submitted, e.g. hashed, document of A_k, who is identified from TSA records, would be employed in an attempt to

regenerate the subsequent, questioned certificate value, C_{k+1}. If that value were correct, D_{k+1} would be proved. As an alternative, the certificate value, C_{k+1}, could be proved by the regeneration of the subsequent catenate certificate value, C_{k+2}, from the certificate data and submitted document of A_{k+2}, since no feasible revision could be made to that later document which would result in a match of C_{k+2} if C_{k+1} were not the same as existed at the time of the transaction, 1330, processing D_{k+2}.

In the more general record catenation procedure depicted in FIG. 5, the documents in a growing series are processed, within an organization or by a TSA, as each is generated. At step 51, a new document representation, such as would be generated by a hashing deterministic function algorithm, becomes available and, at step 52, is concatenated with the current record catenate value that was generated in the processing of the previous document. This composite is then processed, e.g., hashed, at step 53, to generate the new catenate value for the present document. This value may be separately recorded and utilized for inclusion in a certificate, or simply retained in the processing system for application to the next document which is presented at step 54. The subsequent processing steps 55, 56 are applied to this document representation, and the process repeats with each new document in its turn.

What is claimed is:

1. A method for the secure time-stamping of a digital document

c h a r a c t e r i z e d i n t h a t

a) a digital representation of said document is transmitted from an originator to an outside agency;

b) said outside agency creates a receipt comprising a digital representation of then current time and at least a portion of a digital representation of said digital document; and

c) said receipt is certified at said outside agency by means of a verifiable digital cryptographic signature scheme.

2. A method according to claim 1

c h a r a c t e r i z e d i n t h a t

said receipted digital document representation comprises at least a portion of the digital representation of the number derived by application of a deterministic function algorithm to said digital document.

3. A method according to claim 2

c h a r a c t e r i z e d i n t h a t

said digital number representation is derived from the application of a one-way hashing algorithm to said digital document.

4. A method according to claim 1
characterized in that
said receipt further comprises the time representation and digital document representation specific to at least one other digital document receipted by said outside agency.

5. A method according to claim 1
characterized in that
said outside agency is selected at random from a predetermined universe by means of a pseudorandom generator seeded with at least a portion of the digital representation of the number derived from the application of a deterministic function algorithm to said digital document.

6. A method according to claim 5
characterized in that
said pseudorandom generation seed is derived from the application of a one-way hashing algorithm to said digital document.

7. A method according to claim 5
characterized in that
said method further comprises the like preparation of a time-stamp certificate by at least one additional outside agency selected by said pseudorandom generation.

8. A method according to claim 7
characterized in that
said method further comprises the like preparation of a time-stamp certificate by at least one additional outside

agency selected by said pseudorandom generation and wherein the input for each additional outside agency selection is at least a portion of the digital representation of the output derived from the application of said one-way hashing algorithm to a digital representation of the previously generated output.

9. A method of certifying the temporal sequence of digital documents in a series
c h a r a c t e r i z e d i n t h a t
said method comprises:
a) generating a digital representation of a specified one of the documents in said series; and
b) generating a catenate certificate value representation for said specified document by applying a deterministic function algorithm to a concatenation comprising said specified document representation and the catenate certificate value representation for the document next prior in said series to said specified document.

10. A method according to claim 9
c h a r a c t e r i z e d i n t h a t
said method further comprises repeating said recited steps with each subsequent document in said series.

11. A method according to claim 10
c h a r a c t e r i z e d i n t h a t
each said document representation is generated by applying a deterministic function algorithm to said document.

12. A method of time-stamping a digital document which comprises transmitting a digital representation of said document to an outside agency, creating at said outside agency a receipt comprising a digital representation of then current time and at least a portion of a digital representation of said digital document, and certifying said receipt at said outside agency

c h a r a c t e r i z e d i n t h a t

the certifying of said receipt comprises:

a) concatenating a digital representation of said receipt with a representation of a prior catenate certificate value to form a composite; and

b) generating a catenate certificate value for said receipt by applying a deterministic function algorithm to said composite.

13. A method of time-stamping a digital document according to claim 12

c h a r a c t e r i z e d i n t h a t

said outside agency maintains a record comprising the catenate certificate values of prior time-stamping transactions.

14. A method of time-stamping a digital document according to claim 12

c h a r a c t e r i z e d i n t h a t

said receipted digital document representation comprises at least a portion of the digital representation of the value derived by application of a deterministic function algorithm to said digital document.

15. A method of time-stamping a digital document according to claim 14 characterized in that said digital value representation is derived from the application of a one-way hashing algorithm to said digital document.

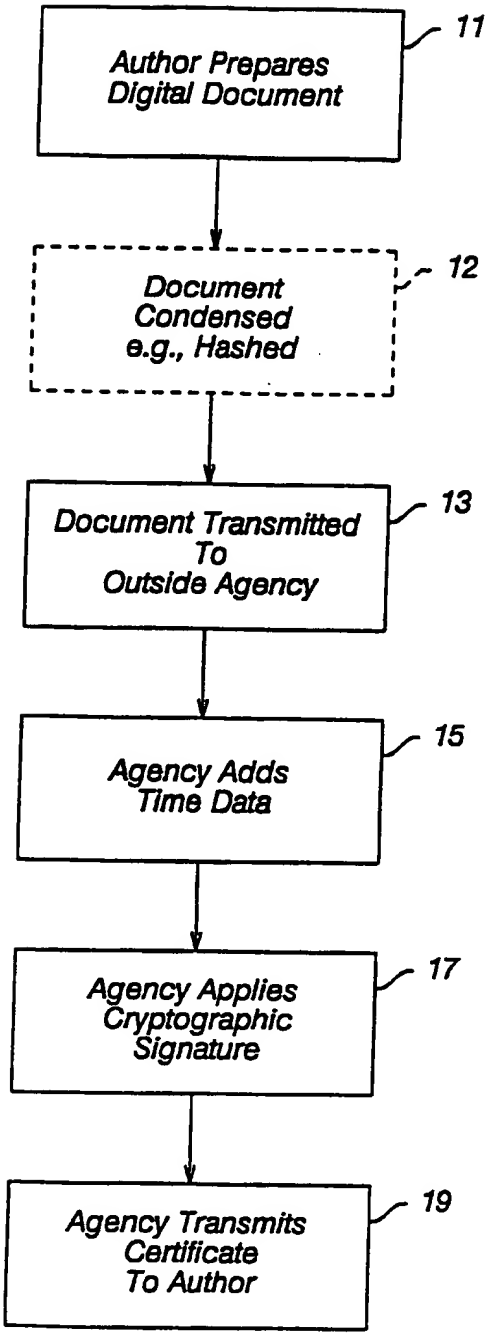

Author Prepares Digital Document
11
Document Condensed e.g., Hashed
12
Document Transmitted To Outside Agency
13
Agency Adds Time Data
15
Agency Applies Cryptographic Signature
17
Agency Transmits Certificate To Author
19

FIG. 1

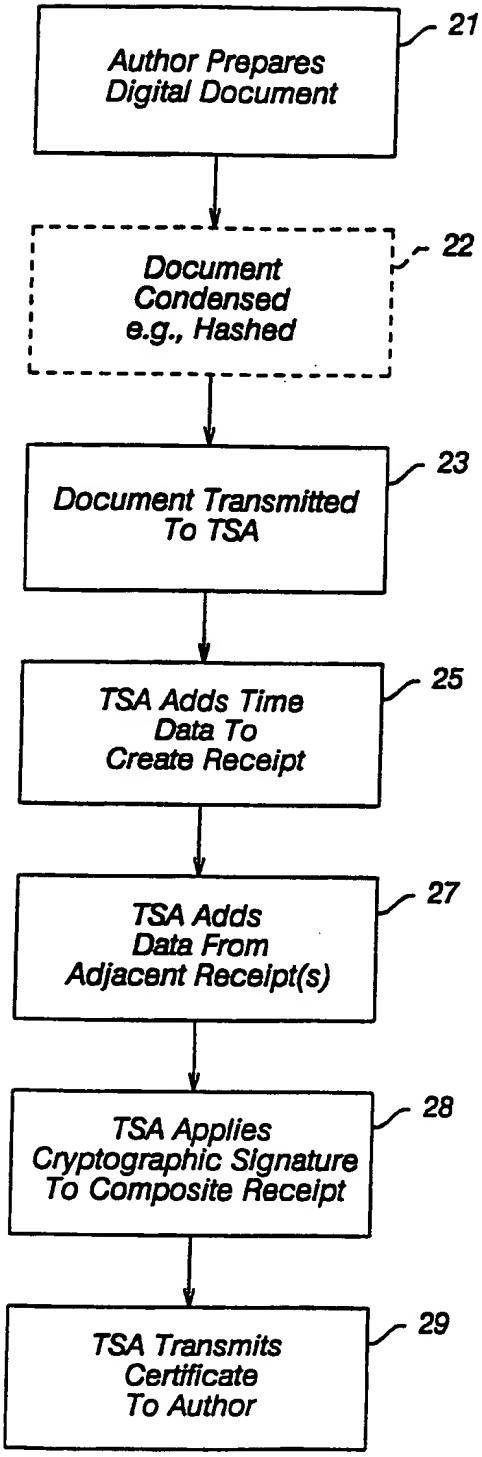

Author Prepares Digital Document
21
Document Condensed e.g., Hashed
22
Document Transmitted To TSA
23
TSA Adds Time Data To Create Receipt
25
TSA Adds Data From Adjacent Receipt(s)
27
TSA Applies Cryptographic Signature To Composite Receipt
28
TSA Transmits Certificate To Author
29

FIG. 2

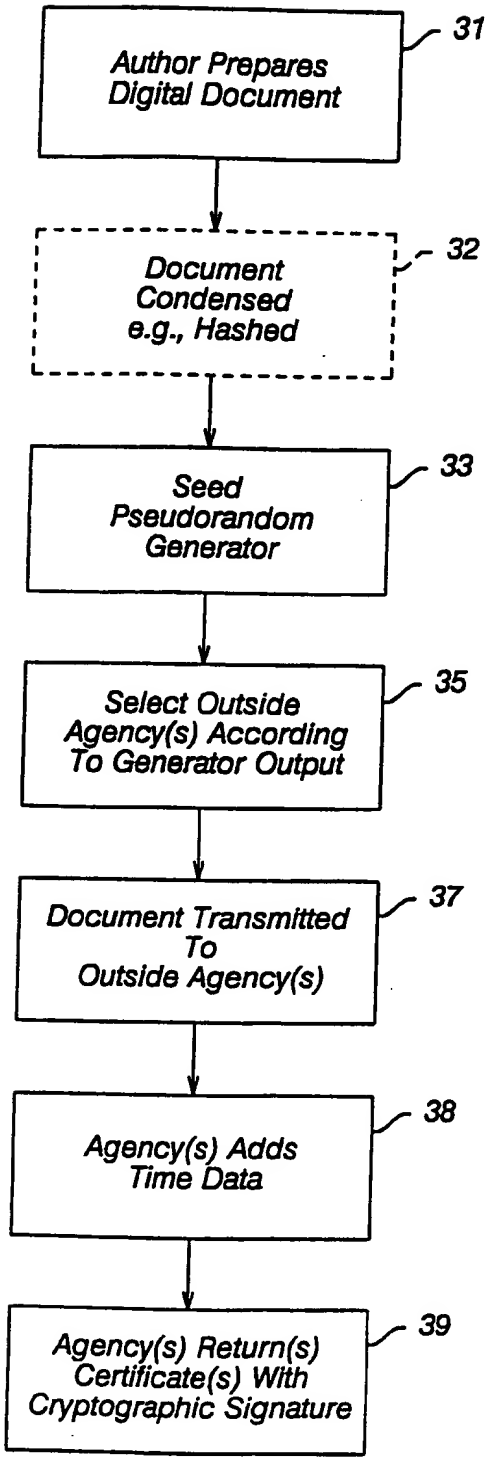

Author Prepares Digital Document
31
Document Condensed e.g., Hashed
32
Seed Pseudorandom Generator
33
Select Outside Agency(s) According To Generator Output
35
Document Transmitted To Outside Agency(s)
37
Agency(s) Adds Time Data
38
Agency(s) Return(s) Certificate(s) With Cryptographic Signature
39

FIG. 3

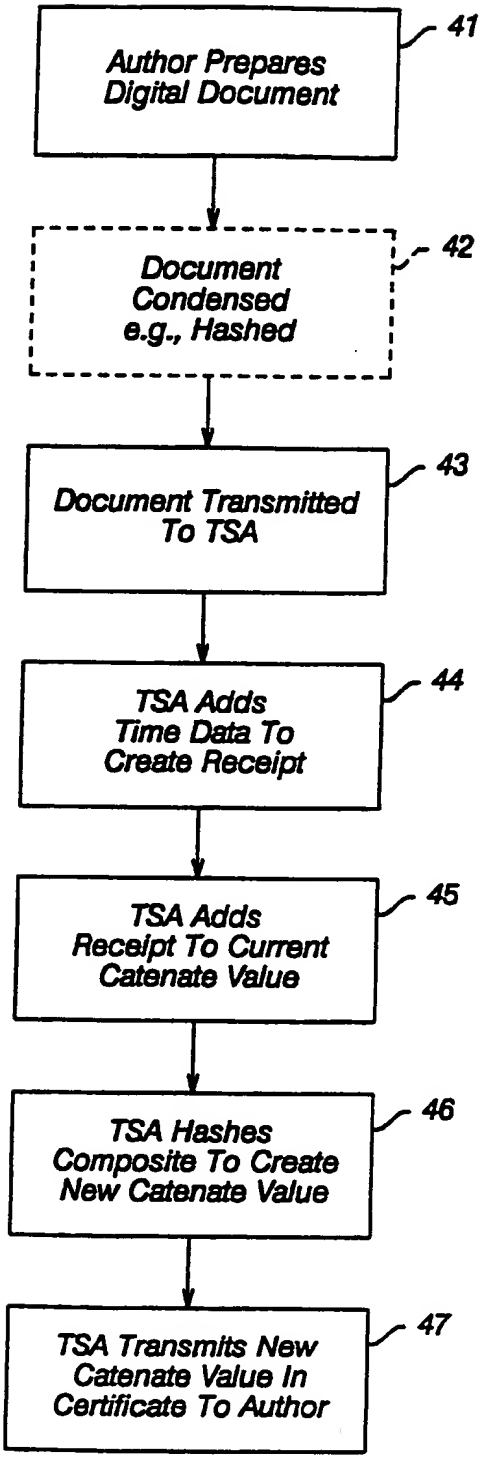

Author Prepares Digital Document
41
Document Condensed e.g., Hashed
42
Document Transmitted To TSA
43
TSA Adds Time Data To Create Receipt
44
TSA Adds Receipt To Current Catenate Value
45
TSA Hashes Composite To Create New Catenate Value
46
TSA Transmits New Catenate Value In Certificate To Author
47

FIG. 4

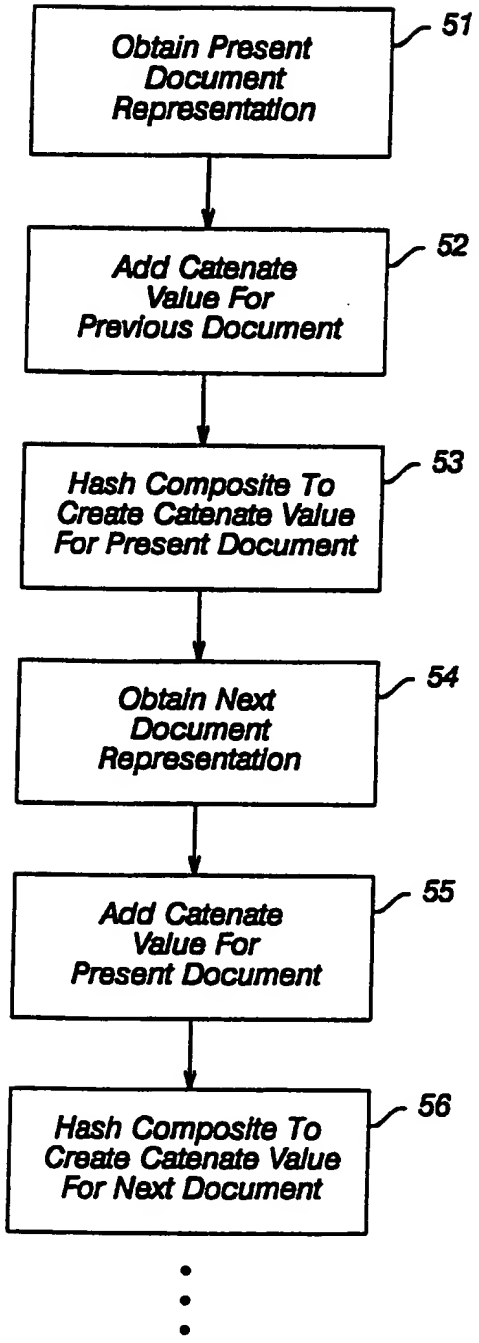

Obtain Present Document Representation
51
Add Catenate Value For Previous Document
52
Hash Composite To Create Catenate Value For Present Document
53
Obtain Next Document Representation
54
Add Catenate Value For Present Document
55
Hash Composite To Create Catenate Value For Next Document
56

FIG. 5

INTERNATIONAL SEARCH REPORT

International Application No. PCT/US91/05386

I. CLASSIFICATION OF SUBJECT MATTER (if several classification symbols apply, indicate all) [6]

According to International Patent Classification (IPC) or to both National Classification and IPC

INT. CL.[5]: H04L 9/00

U.S. CL. : 380/49

II FIELDS SEARCHED

Minimum Documentation Searched [7]

Classification System	Classification Symbols
U.S.	380/4, 23, 25, 30, 49, 50

Documentation Searched other than Minimum Documentation to the Extent that such Documents are Included in the Fields Searched [8]

III. DOCUMENTS CONSIDERED TO BE RELEVANT [9]

Category [10]	Citation of Document, [11] with indication, where appropriate, of the relevant passages [12]	Relevant to Claim No. [13]
A	US, A, 4,145,568 PUBLISHED 20 MARCH 1979, EHRAT.	1-15
A	US, A, 4,206,315 PUBLISHED 03 JUNE 1980, MATYAS ET AL.	1-15

* Special categories of cited documents: [10]

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

IV. CERTIFICATION

Date of the Actual Completion of the International Search	Date of Mailing of this International Search Report
25 OCTOBER 1991	22 NOV 1991

International Searching Authority	Signature of Authorized Officer
ISA/US	For BERNARR EARL GREGORY

INTERNATIONAL DIVISION

Form PCT/ISA/210 (second sheet) (Rev.11-87)

lw 11/16/91